Contents

These are notes for AV's talk in the Mordell seminar on January 22. It talks through most of the ideas of the Mordell proof in the toy case of integral points on $A^2 + B^3 = N$. Note that the extent to which I have checked details is far, far, far lower than in a paper. Use with caution.

1. Introduction

A curve of genus ≥ 2 has finitely many rational points.

Why should we believe this?

If the curve is defined by a complete intersection of degree $(d_1, \ldots, d_k)$ inside $\mathbf{P}^n$, then the genus is ≥ 2 if and only if

$$\sum d_i > n + 1.$$

Now a naive probabilistic argument shows that $f_1(X) = \cdots = f_k(X) = 0$ is likely to have finitely many primitive solutions $X \in \mathbf{Z}^{n+1}$ under the same conditions. This argument gives the generally believed heuristic for higher dimensional varieties: varieties with ample canonical bundle tend to have few points.

In this lecture I'll discuss Faltings' proof, but only in the case of a simple "toy model": finiteness of integral points on $A^2 + B^3 = N$. We study the sequence

If anyone can format this to include the explicit maps, please do so!

(1)

$$\left\{A^2 + B^3 = N : (A, B) \in Z\right\} \to \{\text{elliptic curves with good reduction away from } 6 \cdot N\}$$
$$\xrightarrow{t} \{\text{Galois representations } G_{\mathbf{Q}} \to \mathrm{GL}_2(\mathbf{Q}_2) \text{ unramified away from } 6N\}$$
$$\longrightarrow \{\text{étale cubic } \mathbf{Q}\text{-algebras unramified away from } 6N\}$$

where the elliptic curves, Galois representations and cubic algebras are all taken up to isomorphism. The third and fourth sets will be finite, and the first map has finite fibers; the core of the proof will be to show that t has finite fibers.

We work our way up to this sequence:

- The composite arrow from $\{A^2 + B^3 = N\}$ to cubic algebras amounts to the classical method of *descent*; we discuss it, and explain why the fibers are not easy to understand, in §2.
- In §3 we discuss the map to elliptic curves. This improves descent in that the fibers are easy to understand; one pays the price that it is not clear that the set of elliptic curves good away from $6N$ is not obviously finite.

The proof that t has finite fibers is sketched in the last three sections. The key idea is the construction of the Faltings height (§4), a measure of complexity for elliptic curves or abelian varieties over number fields, and the key technical point is to study how the height varies under isogeny; I give numerical examples in §5. The

basic point of the entire proof is that the height doesn't change too much under isogeny, and I explain the proof in a special case in §6.

2. Warmup: descent on $A^2 + B^3 = N$

I will explain in down-to-earth terms how to do a CM descent on $A^2 + B^3 = N$. This corresponds to making explicit the map from solutions to cubic algebras alluded to in (1).

Set $K_{a,b} := \mathbf{Q}[x]/(x^3 + 3ax + 2b)$ Then

$$(*) \quad \mathrm{disc}(K_{a,b}) = \frac{-108(a^3 + b^2)}{\square}.$$

The map $a, b \mapsto K_{a,b}$ gives

$$\{A^2 + B^3 = N\} \longrightarrow \text{cubic } \mathbf{Q}\text{-algebras of discriminant dividing } 108N.$$

The right-hand side is finite by Hermite-Minkowski theorem.

What of the fibers? Fix an étale $\mathbf{Q}$-algebra A with ring of integers $\mathfrak{o}_A$ (= integral closure of $\mathbf{Z}$ in A). To each solution (A, B) with $\mathbf{Q}[x]/(x^3 + 3ax + 2b) \cong A$ the image of x under such an isomorphism gives an element $a \in \mathfrak{o}_A$ of trace 0 with $\mathrm{disc}(a) = -108N$. Now there exists a unique, up to sign, cubic form $P : \mathfrak{o}_A^0 \to \mathbf{Z}$ so that $\mathrm{disc}(a) = \mathrm{disc}(A) \cdot P^2$; here $\mathfrak{o}_A^0$ consists of elements with trace 0. Consequently *the fibers of the map (*) above A are given by solutions to $P = \sqrt{N/\mathrm{disc}(A)}$, where P is a binary cubic form;* we have traded one cubic equation in two variables for another; this is an explicit example of *descent*.

There is indeed an explicit map of degree three

$$\left\{ a \in \mathfrak{o}_A^0, P(a) = \sqrt{\frac{N}{\mathrm{disc}(A)}} \right\} \longrightarrow \left\{ A^2 + B^3 = N \right\}$$

which sends a to its characteristic polynomial. Over an algebraic closure this becomes isomorphic to the degree 3 self-isogeny of $y^2 + x^3 = 1$.

Example: $N = -21$. We will show there are no solutions.

There are no cubic fields whose discriminant is of the form $\frac{108 \times 21}{\square}$, and the algebras with this discriminant are therefore $\mathbf{Q} \oplus L$ where L is a quadratic field of discriminant dividing $108 \cdot 21$. We may write elements of $\mathfrak{o}_L$ as $\frac{p + q\sqrt{\Delta_L}}{2}$ with $p, q \in \mathbf{Z}$ – possibly subject to a congruence constraint at 2 – and then

$$\mathrm{disc}(-p, \frac{p + q\sqrt{\Delta_L}}{2}) = \left((9p^2 - q^2\Delta_L)q/4\right)^2 \Delta_L.$$

Consequently we are reduced to solving the equation

$$q(9p^2 - q^2\Delta_L) = \sqrt{\frac{108 \cdot 21}{\Delta_L}}$$

for each quadratic field L of discriminant $\frac{108 \cdot 21}{\square}$ and one easily checks there are no solutions. Clearly this method works whenever there are no cubic fields of discriminant $-\frac{108N}{\square}$: descent yields another cubic but one that is much easier to solve because it factors.

Example: $N = 19008$.

There are four cubic fields whose discriminant is of the form $\frac{-108N}{\square}$; they are, respectively, K, L, M_1, M_2 generated by roots of $x^3 - x^2 + x + 1, x^3 + 6x - 1, x^3 +$

$6x - 10, x^3 - 12x - 28$; they have discriminants $-44, -891, -3564, -3564$ (not a typo).

Here are the solutions I found for $|B| < 10^6$, together with $K_{a,b}$:

$$(-375376, 229985128, K), (-5448, 402120, M_1), (-201, 2853, L),$$
$$(-192, 2664, M_2), (-136, 1592, K), (-48, 360, M_1),$$
$$(-16, 152, K), (-12, 144, L), (8, 136, K), (24, 72, M_2).$$

Here's a sample of the descent: a corresponding computation shows that the fiber of $(a, b) \mapsto K_{a,b}$ above L is identified with solutions of

$$-2x^3 + 6x^2y - 4xy^2 + y^3 = -216,$$

which has the solution $(618, 282)$ beyond the obvious solution $(0, -6)$. Incidentally, the elliptic curve $y^2 = x^3 + 19008$ has rank 2: it is the curve 13068K2.

* * *

We now interpret the foregoing in more abstract terms. The equation $A^2 + B^3 = N$ defines a curve Y; considering $x^3 + Ax + B = 0$ defines a *three-fold cover* of this curve $\tilde{Y} \to Y$.

Our point is that the preimage of an integral point on Y must be defined over a very small set of fields: the covering $\tilde{Y} \to Y$ describes a map

$$(a, b) \in Y(\mathbf{Z}) \longrightarrow K_{a,b} \in \{ \text{ cubic fields}\}. \tag{2}$$

This is the basic idea of *descent*: coverings of a variety inhibit the existence of rational points because of the *finiteness of fields with fixed degree and discriminant.* The basic problem is that it is not at all clear that many different points on X might give rise to the same field, i.e. the fibers might be infinite. This leads us to the first idea in Faltings' proof, namely, one can "enrich" this process by considering a richer object than cubic fields.

3. $A^2 + B^3 = N$: enriched descent

We will now "enrich" the previous discussion as promised: Instead of associating to a solution the algebra $\mathbf{Q}[x]/(x^3 + ax + b)$, we consider the *elliptic curve* $y^2 = x^3 + 3ax + 2b$. The discriminant of this elliptic curve divides $-1728(a^3 + b^2)$. In terms of the discussion around (2): instead of considering the finite covering $\tilde{Y} \to Y$ we consider the map $\mathcal{E} \to Y$ with fibers elliptic curves.

This (more or less) fixes the failure of injectivity: $E_{a,b} \cong E_{a',b'}$ if and only if $b^2/a^3 = b'^2/a'^3$. This is a strict "enrichment" of what went before: we recover $K_{a,b}$ by considering the 2-torsion. So finiteness will follow from

$$\boxed{\text{Finiteness of elliptic curves with given discriminant.}}$$

For abelian varieties the analogue was conjectured by Shafarevich. Although Shafarevich gave a proof for elliptic curves, Faltings gave a *totally different proof that generalized to abelian varieties*; this is the engine of the proof of Mordell.

In the prior section we studied the map

$$\{(A, B) : A^2 + B^3 = \dots\} \longrightarrow \{\text{cubic algebras}\},$$

which sends (A, B) to $K_{A,B} = \mathbf{Q}[x]/(x^3 + 3Ax + 2B)$. The set of cubic fields is finite. But the fibers are mysterious. We have now "factored" the map f as:

$$\{(A, B) : A^2 + B^3 = \dots\} \xrightarrow{e} \{\text{elliptic curves}\} \xrightarrow{f} \{\text{cubic fields}\}$$

where e has finite fibers, and the map f is given by extracting 2-torsion.

A key idea in Faltings' proof is to factor this further by considering the Galois representation on all the 2-power torsion, i.e. the associated Galois representation $G_{\mathbf{Q}} \longrightarrow \mathrm{GL}_2(\mathbf{Q}_2)$ given by the representation[1] on the Tate module $T_2E \otimes_{\mathbf{Z}_2} \mathbf{Q}_2$. Thus we have expanded our original picture:

$$\{A^2+B^3=N\} \to \{\text{elliptic curves}\} \xrightarrow{t} \{\text{Galois representations}\} \longrightarrow \{\text{cubic fields}\}$$

The proof of finiteness passes from cubic fields to Galois representations. That is to say, there are only finitely many Galois representations $G_{\mathbf{Q}} \to \mathrm{GL}_2(\mathbf{Q}_2)$, unramified away from primes dividing N, and so that every Frobenius Fr_p has trace an integer between $-2\sqrt{p}$ and $2\sqrt{p}$. This is "elementary", using only Chebotarev, but ingenious.

We're reduced to checking that:

$$\boxed{t \text{ has finite fibers.}}$$

* * *

Let us now discuss how this setup generalizes to the Mordell context. The only specific feature of $Y : A^2 + B^3 = N$ that was used was the existence of the elliptic family $E_{A,B} \to Y$. The existence of such families is not an accident; there is a systematic way due to Kodaira–Parshin of constructing them, and the proof of the Mordell conjecture one uses the following variant:

> Given any projective curve X of genus ≥ 2, there is a "non-trivial" abelian variety over X.

In other words, any projective curve admits a nonconstant morphism to the moduli space of abelian varieties. This is rather amazing to me. This then reduces the problem of finiteness of rational points on X to

> Finiteness of the number of (p.p.) abelian varieties with bad reduction at a fixed set of places.

I should describe how to associate to any $x \in X$ an abelian variety A_x. The short answer is "take the Jacobian of a cover branched only at x." There may be several, so to resolve ambiguity take the *product of the Jacobians of all the* 3*-fold branched coverings of* X*, branched only at* x.

Example. Suppose we did not know about the family $E_{A,B}$ over $E : A^2+B^3 = N$. We could use the Kodaira-Parshin construction to construct a substitute as follows:

For P a point on E, there are exactly 4 pairs $(X, f : X \to E)$ of a hyperelliptic curve X and a degree 2 map f, branched only at 0 and P. For each one the Jacobian $\mathrm{Jac}(X)$ maps naturally to E and the kernel is another elliptic curve E'. The product $\prod E'$ gives an abelian variety of dimension 4 over the complement of the identity in E, and the previous discussion goes through using this family instead of $E_{A,B}$.

We can be quite explicit: the four curves E' associated to a point P on E are exactly the four double coverings of $\mathbf{P}^1$ ramified at $x(P/2)$ and three of $\{x^3 - N = 0\} \cup \{\infty\}$. (Here $x(P/2)$ is the x-coordinate of any point which doubles to P; the result is independent of choice.)

---

[1]There is a choice about what 2-adic representations means: we could consider $T_2(E)$ or $T_2(E) \otimes \mathbf{Q}_2$. The latter is a little bit cleaner because the fibers will turn out to be exactly isogeny classes, but this is not major point.

4. The Faltings height

We are reduced to showing that the map t of

$$\{\text{elliptic curves}\} \xrightarrow{t} \{\text{Galois representations } G_{\mathbf{Q}} \to \mathrm{GL}_2(\mathbf{Q}_2)\ \},$$

associating to any elliptic curve its Tate module, has finite fibers. There are two steps:

R1. *Tate conjecture.* The fibers of t consist of isogeny classes;
R2. Isogeny classes are finite.

In fact, (R2) implies (R1) – or, more precisely, knowing the analog of (R2) for all abelian varieties implies (R1). This is an argument of Tate, to be reprised by Sam.

To each elliptic curve E over $\mathbf{Q}$ Faltings assigns a "height" $\hat{h}(E) \in \mathbf{R}_{>0}$. This height has two critical properties:

F1. There are finitely many curves, up to isomorphism, of bounded Faltings height.
F2. The height "does not change much under isogeny"; in particular, the height is bounded above in any isogeny class.

Clearly (F1) + (F2) $\Longrightarrow$ (R2). Now part (F2) is the absolute core of the whole business (although (F1) is not easy, I think (F2) is "less intuitive") so I'll repeat it.

The Faltings height does not change much under isogeny.

Now we construct this $\hat{h}$.

* * *

Given an elliptic curve E and a 1-form ω on E there is a unique lattice $\Lambda \subset \mathbf{C}$ so that there is a (unique) isomorphism

$$(E, \omega) \cong (\mathbf{C}/\Lambda, dz).$$

Λ is the "period lattice."

If E is defined over $\mathbf{Q}$, one can normalize ω up to $\mathbf{Q}^\times$ by demanding that it is "defined over $\mathbf{Q}$"; the theory of the Weierstrass minimal model (more generally: Néron model) in fact normalizes ω_N up to $\mathbf{Z}^\times = \{\pm 1\}$. This in particular normalizes the period lattice, and the *Faltings height* is defined to be[2]

$$\hat{h} := \mathrm{area}(\mathbf{C}/\Lambda_N)^{-1}.$$

In practice, write E in the form $y^2 = x^3 + Ax + B$ where there doesn't exist a prime p with $p^3|B, p^2|A$; this is possible because we can rescale $(A, B) \leftarrow (A/z^2, B/z^3)$. By complex analysis there is a lattice Λ so that $A = 15G_4, B = 35G_6$, and indeed $(\mathbf{C}/\Lambda, dz) \cong (E, \frac{dx}{2y})$. Then $\hat{E}$ differs from a bounded amount from $\mathrm{area}(\mathbf{C}/\Lambda)^{-1}$. In fact

$$\hat{h}(E) = \mathrm{area}(\mathbf{C}/\Lambda)^{-1} \cdot (\Delta_{min}/\Delta)^{1/6}$$

and with the above choice of $(A, B) \in \mathbf{Z}$, we have $\frac{\Delta}{\Delta_{min}} \leq 1728$.

Some numerical examples:

- $y^2 = x^3 + 11x + 14$. This is already minimal, and the Faltings height is about 0.54.
- $y^2 = x^3 + 111x + 114$ has Faltings height about 1.54;

[2]There are various ways to normalize (square root, logarithm).

- $y^2 = x^3 + 1111x + 1114$ has Faltings height about $4.85\ldots$.

* * *

Now about (F1): why finitely many elliptic curves with $\hat{h} \leq X$?

Choose a model $y^2 = x^3 + Ax + B$ with $\Delta/\Delta_{min} \leq 1728$ and let Λ be the period lattice for $(y^2 = x^3 + Ax + B, \frac{dx}{y})$. Then $\text{area}(\mathbf{C}/\Lambda) \geq 1728/X$.

The basic principle at work is that Λ *cannot be too skew because* $|\Delta(\Lambda)| \geq 1$*:*

Let $a < b$ be the lengths of vectors in a reduced basis for Λ. The fact that $|\Delta| \geq 1$ implies $b/a \ll \log X$. On the other hand, $(ab) \asymp 1/X$. Thus $a \gg \frac{1}{\sqrt{X}\log X}$, which implies that A, B are bounded by X^2, X^3 up to powers of $\log X$.

Exercise. Compute the Faltings height of the curve $y^2 = x^3 + D$ (with particular reference to variation of D).

5. Isogeny and heights

We return to discussing the boxed statement: *the Faltings height doesn't change much under an isogeny.* This section is devoted to numerical examples – I'll describe how to compute them later – and the next section will briefly discuss the proof.

At first glance the examples are in the wrong direction: they suggest that the height *can* change under isogeny. But the purpose of this section is just to show how heights interact with isogeny; in the next section we'll explain that the type of situation which forces the height to change "can only occur finitely often."

Example. There are three elliptic curves of conductor 11:

$X_1(11)$: $y^2 + y = x^3 - x^2$
$X_0(11)$: $y^2 + y = x^3 - x^2 - 10x - 20$
$\bar{X}$: $y^2 + y = x^3 - x^2 - 7820x - 263580$.

Note that, after transforming into the form $y^2 = x^3 + Ax + B$, $\bar{X}$ corresponds to the big solutions to $A^2 + B^3 = 19008$ presented earlier. $X_1(11)$ gives the solution $(-16, 152)$.[3]

PARI will tell you the period lattice of $X_1(11)$ as `e.omega` $= [6.3460, -3.1730 + 1.4588*I]$. It also tells you the Faltings height $X_1(11)$ equals `e.area`$^{-1} \approx 0.108$. The Faltings height of $X_0(11)$ equals $\approx 0.540\ldots$. The Faltings height of $\bar{X}$ is ≈ 2.70. Thus – as we see "naively" from the minimal models – the Faltings height increases as we pass from $X_1(11)$ to $X_0(11)$ to $\bar{X}$.

Thus we have 5-isogenies

$$X_1(11) \longrightarrow X_0(11) \longrightarrow \bar{X}$$

each one quintupling the Faltings height; their kernels are given by $(1, -1)$ and $(16, -61)$; in the dual direction

$$\bar{X} \longrightarrow X_0(11) \longrightarrow X_1(11)$$

at each stage divides the Falting height by 5 and the kernels are generated by points with x-coordinate respectively roots of $5\alpha^2 + 5\alpha = 29$ and $5\alpha^2 + 505\alpha + 12751 = 0$. Note that both of these lie in $\mathbf{Q}(\sqrt{5})$. In fact, the action of $G_{\mathbf{Q}}$ on the kernel of the isogeny is by the cyclotomic character valued in $(\mathbf{Z}/5\mathbf{Z})^\times$.

Example. There's an isogeny between

$$y^2 + (x+1)y = x^3 - x^2 - 3x + 3 \to y^2 + (x+1)y = x^3 - x^2 - 213x - 1257.$$

[3] $X_0(11)$ doesn't give such a solution; its discriminant is -11^5.

The isogeny has kernel $(3, -6)$. The kernel of the dual isogeny is generated by $(\alpha, -)$ where α is a root of $7x^3 + 105x^2 - 658x - 7237$ and lies in the cubic field of discriminant 49. In fact the action of $G_{\mathbf{Q}}$ on the kernel of the dual isogeny is via the cyclotomic character valued in $(\mathbf{Z}/7\mathbf{Z})^\times$.

Based on this data and the ability to draw dubious conclusions from grossly inadequate evidence, we come to the provisional conclusion:

Isogenies raise heights when the kernel is generated by a rational point.

This is not quite right – it's clearly false for 2-isogenies, for instance – but its heart is in the right place. A precise statement along these lines is found in the next section; it's exactly true when the curve has squarefree conductor and the isogeny is of odd prime order, for instance.

Nonexample. In the example

$$\{A^2 + B^3 = 19008\} \leftarrow \{-2x^3 + 6x^2y - 4xy^2 + y^3 = \pm 216\}$$

the left-hand curve has height ≈ 1.31, the right-hand ≈ 0.44; neither of the isogenies have kernel generated by a rational point, for neither curve has any rational torsion. The problem is this: these curves are far from *semistable*.

Practical comments about the computation:

(i) How would we know that there is this 25-isogeny out of $X_1(11)$? Let $a(p)$ be the pth coefficient of the L-series, i.e. the pth coefficient of

$$q\prod((1-q^n)(1-q^{11n}))^2.$$

Not only is the mod 5 Galois representation reducible, as attested to by the fact that

$$a(p) \equiv p + 1 \bmod 5,$$

but also the mod 25 Galois representation is reducible, as one can see from

$$a(p) \equiv p\chi(p) + \chi(p)^{-1} \bmod 25,$$

where $\chi(p) = 1 + 5\psi(p)$, and $\psi : (\mathbf{Z}/11)^\times \longrightarrow (\mathbf{Z}/5)$ sends 2 mod 11 to 1.

Note that this alone uniquely determines $a(p)$ for $p < 156$. It gives a congruence modulo 25 between E and an Eisenstein series of level 121.

(ii) How do we find the kernel of the isogeny (or the equations for the isogenous elliptic curves)?

I would do this via complex-analytic uniformization: One checks all six sublattices of a period lattice and looks for algebraicity of G_4, G_6.

6. The core of the proof that the height doesn't change much under isogeny

Suppose that $f : E \to E'$ is an isogeny betweem *semistable* abelian varieties – for elliptic curves this means "squarefree conductor" – whose kernel is isomorphic to $(\mathbf{Z}/\ell\mathbf{Z})^k$. Suppose moreover that E has good reduction at ℓ.

The Galois group acts on the kernel:

$$\rho : G_{\mathbf{Q}} \to \mathrm{GL}_k(\mathbf{Z}/\ell\mathbf{Z}).$$

By semistability, $\det\rho$ is ramified only at ℓ. By class field theory, it's a power ω^h of the cyclotomic character valued in $(\mathbf{Z}/\ell\mathbf{Z})^\times$, where $0 \le h \le \ell - 2$. Here is then the basic fact:

The height changes by a factor $\frac{\hat{h}(E')}{\hat{h}(E)} = \ell^{k-2h}$.

This innocuous-looking statement is a local computation at ℓ, but requires the classification of finite flat group schemes over $\mathbf{Z}_\ell$ due to Raynaud (this fails at $\ell = 2$).

Examples:

- Multiplication by ℓ on an elliptic curve E: here $h = 1, k = 2$, $\frac{\hat{h}(E')}{\hat{h}(E)} = 1$.
- ℓ-isogeny $E \to E'$, ker generated by rational point: $h = 0, k = 1$, $\frac{\hat{h}(E')}{\hat{h}(E)} = \ell$.
- Dual of the previous situation: $h = 1, k = 1$, $\frac{\hat{h}(E')}{\hat{h}(E)} = \ell^{-1}$.

Now let p be a small fixed prime at which E has good reduction; the action of F_p on $T_\ell E$ has all eigenvalues reductions of Weil number of absolute value $p^{k/2}$. One deduces that *for large enough* ℓ that

$$h = k/2.$$

For elliptic curves this shows that ℓ-isogenies simply don't exist for large ℓ. Iin general there can certainly be many isogenies $E \to E'$ with ℓ-group kernel, and the argument says nothing about them beyond the invariance of height.

Warning: One needs a separate argument for small ℓ! The argument above was for large enough ℓ. Thus it controls isogenies of degree divisible only by "large" primes; but it says nothing, for example, about heights under isogenies of degree 2^{1000}. For small ℓ, one replaces the above argument with a somewhat similar argument, but using Tate's results on p-divisible groups instead of Raynaud's results on finite flat group schemes.